Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Bucharest, September 2020

Regional Study on Personal Data Protection aspects of law enforcement action on cybercrime in the Eastern Parrneship region

Contacts

Giorgi.Jokhadze@coe.int
Cybercrime Programme Office of the Council of Europe (C-PROC)
Bucharest, Romania

Disclaimer

This document has been produced as part of CyberEast, a project co-funded by the European Union and the Council of Europe, with inputs from experts Marko Juric (Zagreb University, Croatia) and Markko Kunnapu (Ministry of Jusitce, Estonia). The views expressed herein can in no way be taken to reflect the official opinion of either party.

Contents

LIST OF ABBREVIATIONS

CJEU – Court of Justice of the European Union

CoE – Council of Europe

Convention 108 - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

Convention 108 Amending Protocol or **Amending Protocol** - 2018 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

ECHR – European Convention for the Protection of Human Rights and Fundamental Freedoms

ECtHR – European Court of Human Rights

EU – European Union

GDPR - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88

Law Enforcement Directive - Directive (EU) 2016/680 on the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data.

LEAs – Law enforcement agencies

1 Introduction

The aim of the present report is to provide an overview on standards related to personal data protection and its use in criminal proceedings in the Eastern Partnership region.

The report covers Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine.

All the countries listed above except Belarus are parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).[1]

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No.223)[2] was opened for signature on 10.10.2018. As of July 2020 only Armenia has signed the protocol.

Belarus, although not a party to the convention is still working on order to bring its legislation in line with international standards, such as the Convention 108 and European Union General Data Protection Regulation (GDPR)[3] and Police Directive.[4]

The standards related to personal data protection have become more important than ever before and need to be respected also by law enforcement authorities. Although there are data protection related exceptions in place for the law enforcement and criminal investigations, the main data protection principles still need to be followed. As evidence in the criminal proceeding often contains personal data, these standards need to be borne in mind.

In addition to criminal investigations at domestic level and cooperation with public and private sector entities, attention has to paid to international cooperation as well. Rules and limitations related to further use of data and onward transfers must be respected.

In case of international cooperation and cross-border personal data transmission, sending or receiving personal data, certain conditions and safeguards must be met. In order to cooperate effectively, both requesting and requested country must have minimum standards on data protection in place. If a country requesting personal data doesn't have necessary or adequate data protection regime in place, additional conditions and safeguards as well as limitations apply.

Although the Cybercrime Convention or Budapest Convention[5] has minimum standards on both substantive law and procedural law as well as legal basis for international cooperation, it doesn't provide for specific standards on data protection.

---

[1] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

[2] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
https://eur-lex.europa.eu/eli/reg/2016/679/oj

[4] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680

[5] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

However, the data protection instruments mentioned above will still be applicable. Countries who are parties to Convention 108 need to apply the standards of the Convention, while those who are bound by European Union law and GDPR will need to respect requirements of the latter.

This means that in order to cooperate with other countries, they should also have certain minimum standards in place, otherwise the cooperation would be less effective. If the receiving country doesn't have sufficient standards in place, transmission of evidence, computer data containing personal data might not be possible.

On 10.10.2018 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223)[6] was opened for signature. As of June 2020, the Protocol hasn't entered into force.

In 2017 negotiations on the Second Additional Protocol to the Budapest Convention[7] started and the finalization of the work is expected by the end of 2020.

As one of the key elements of the Second Additional Protocol is data protection standards as well as conditions and safeguards related to cross-border personal data flows, countries need to take it seriously and implement relevant international standards as soon as possible. If relevant standards are not fully met, it could have a negative impact on the international cooperation.

[6] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223

[7] https://www.coe.int/en/web/cybercrime/t-cy-drafting-group

2 Armenia

2.1 Introduction

Armenia has ratified the Convention 108 on 9 May 2012. It has also signed the Amending Protocol on 2 October 2019.

Standards related to protection of personal data have been provided by the Constitution of the Republic of Armenia and Law on Personal Data Protection.

Personal Data Protection Agency under the Ministry of Justice has been designated as competent data protection authority.

2.2 Legislation

The Constitution

The safeguards related to private life, secrecy of communications and protection of personal data are provided by Articles 31, 33 and 34 of the Constitution.

Pursuant to Article 31 private and family life may be interfered with if provided by law and for the purposes of state security, economic welfare of the country, preventing or disclosing crime, protection of public order, health and morals or the rights and freedoms of other persons.

Similar conditions are required also by Article 33 on the restriction of secrecy of communications.

Protection of personal data has been addressed by separate Article 34 which guarantees everyone a right to protection of personal data. The processing of personal data must be carried out in good faith and for the purpose provided by law. The processing is based on the data subjects' consent except for the cases foreseen by law. Everyone has a right to access personal data related to him or her, as well as request correction or deletion of data. Access to personal data may be restricted by law and for the purposes mentioned earlier. Article 34 also requires that details related to the protection of personal data must be provided by law.

Criminal Procedure Code

The Criminal Procedure Code of Armenia (AmCPC) doesn't contain specific provisions on processing and protection of personal data. However, to some extent protection of personal data is covered by general provisions and safeguards as well as procedural rights.

According to Article 9 the respect of rights and freedoms as well as dignity of a person is mandatory for all bodies and persons participating in criminal proceeding.

Article 14 ensures the right to a confidentiality of communications and restriction is allowed only if prescribed by law and permitted by the court.

Pursuant to Article 16 the court trials are held in public. However, to protect the private life trial can be held *in camera*. Court verdicts and final decisions are announced publicly.

The AmCPC has also specific provision related to confidentiality of personal data. Pursuant to Article 170, the collection and processing of data related to personal or family life is not allowed while carrying out the court actions. Disclosure of information is not allowed. Moreover,

information related to intimate aspects of personal and family life must be discussed at closed court sessions.

Although the AmCPC has several provisions on protection of private and family life, there are no provisions on processing the personal data and exceptions for criminal procedure purposes. Also, Article 170 could be misleading, because evidence gathered during the pre-trial proceeding and presented later in court could also contain personal data.

Law on Personal Data Protection

Armenian Law on Personal Data Protection (AmLPDP) provides the procedure and conditions related to personal data protection as well as exceptions.

Article 1 provides for the scope of the law and covers data processing by public and private sector. However, it has very broad exception with regard to different categories of data such as data related to official, banking, notarial, insurance secrecy, legal professional privileges, if being used for national security or defence, fight against money laundering and terrorism, operational-intelligence activity purposes. There is a general reference that these proceedings will be regulated by other laws. The law also excludes processing of personal data for journalism, literary and artistic purposes. Unlike many other laws, there is no reference for cases where data is being used for personal purposes.

There is also a reference that supervision and control related to personal data may be prescribed by other laws and different bodies could be in charge.

Article 3 provides for the main definitions including personal data, processing of personal data, processor of personal data and data transfers. There is also a specific definition on information system that relates to set of personal data in the database and information technologies or technical means used to process data. The law also introduces specific categories of personal data such as data on personal life, biometric personal data, special category personal data and publicly available personal data.

According to the law personal data processing must comply with the requirements and principles provided by the law. The principles that have been introduced are lawfulness, proportionality, reliability and minimum engagement of a data subject.

There is a general rule that processing of personal data must comply with the law and consent of the data subject must be present unless the data processing is foreseen by laws. It is also lawful to process data that has been obtained from publicly available sources.

The law also provides for the rights of a data subject and obligations for a data processor. Data subject has also a right to appeal on the actions or inactions of the data processor.

As it has been provided by Article 1 of the law, there can also be different bodies exercising control over processing of personal data. Article 22 explains the procedure and coordination between different bodies. However, in case of criminal proceedings the procedures are not clear and the law doesn't say explicitly which authority is in charge and whether Data Protection Authority has also a role or function in the criminal proceedings.

Article 23 contains an obligation to notify Data Protection Authority about the processing of personal data. Still it remains unclear whether this obligation would apply also to situations where data is being processed on the basis of law, such as processing by criminal justice authorities.

Articles 26 and 27 set the conditions for transfer of personal data to third parties and other states.

The transfer may take place if there is a consent of a data subject. It can also take place if the transfer is needed for the purposes of the processing of personal data. If transfer is to another state, then the permission of Data Protection Authority is needed unless the other state as an adequate level of personal data protection in place. Adequate level of protection is assumed where data is being transferred in compliance with international agreements or where country has been included in a special list published by Data Protection Authority.

As Armenia is party to the Convention 108 then it can be deducted that all other parties to the same Convention are considered as adequate. However, the law doesn't specify how and based on which criteria the list of other countries is created.

There are also exceptions for countries which are not considered as adequate in terms of personal data protection. In this case, the permission of the Data Protection Authority is needed and the prerequisite is an agreement with a country providing necessary safeguards. The processor of personal data needs to obtain the permission prior the data transfer and Data Protection Authority may refuse the transfer.

The list of countries to whom data can be transferred is updated not less than once in a year and published.

Data transfer to foreign state bodies may take place only within the framework of interstate agreements. As regards transfer to non-state bodies then the law would apply.

Although the law has in place conditions and safeguards to transfer personal data to another state, it can still be considered as very limited. For instance, there are no provisions and exceptions for cases where personal data need to be transferred to another country, international organisation or private entity in order to protect public interests or interests of the data subject.

2.3 Data protection authority

Pursuant to Article 24 of the AmLPDP the protection of personal data shall be carried out by the authorised body designated by the government.

In Armenia, the authorised body or data protection authority is the Personal Data Protection Agency under the Ministry of Justice. It is a separate division of the Ministry and its powers and functions have been provided by international treaties and domestic legislation.

The authorised body of Data Protection Agency supervises the implementation and application of the law and *inter alia* checks the compliance of the processing of personal data, applies administrative sanctions, gives order to processors of data including on prohibition of processing.

It also is responsible for the recognition of electronic systems for processing personal data and checking the devices including computer software.

There is also a reference related to reporting to law enforcement bodies if there is a suspicion of a criminal offence.

However, there are no more provisions or references to criminal justice authorities and related processing of personal data. Although the law obliges the Data Protection Authority to check the validity and give permission to cross border data transfers to a non-adequate country, it doesn't provide detailed procedures and criteria.

3 Azerbaijan

Deleted on request of authroties of Azerbaijan.

4 Belarus

4.1 Introduction

Belarus is not a Member State of the Council of Europe and not Party to the Convention 108.

The Constitution of Belarus provides for general safeguards related to protection of private life. Law on Information covers general matters related to databases and access to information. However, it has also few provisions on protection of personal data.

There is no specific personal data protection authority.

At the moment, there is no specific legislative act on personal data protection in place. However, the authorities are working on the matter and draft law has been prepared.

4.2 Legislation

The Constitution

The Constitution of Belarus provides for the basic rights and freedoms, including protection of private life, state obligation to ensure the implementation of those and necessary remedies, which include a right to go to the court.

According to the Articles 23 any restriction of personal rights and freedoms must be permitted by the law. Article 28 provides that everyone shall have the right to protection against unlawful interference with the private life, including privacy of the correspondence and communications.

The state has an obligation to ensure the protection of the rights and freedoms. Pursuant to Article 59 state bodies, officials and other persons entrusted to exercise state functions shall within their competence take necessary measures to implement and protect personal rights and freedoms. Article 60 allows everyone to seek remedies and submit claims to the court.

Law on information, informatization and protection of information

The main aim of the law is to provide a legal basis for public sector databases, processing the data and enabling access to them.

Although the primary focus is not to establish legal framework on personal data protection, it still contains few provisions related to the definition and protection of personal data.

Article 1 contains the definition of personal data. Personal data are data on physical persons in the population register as well as data enabling identification of a particular individual.

According to Article 15, access to information depends on the category of data and whether it is in the public access or restricted access. Pursuant to Article 17, access is restricted to data related to private life of and individual and personal data. Basic protection has been provided by Article 18, according to which it is not allowed to demand an individual to disclose information on his/her private life or obtain this information without his/her consent, unless it is provided by the law. Procedures related to processing of personal data have to be provided by law.

Article 27 provides for the general rules on protection of data, including the ensuring the confidentiality, integrity and availability of data. It also covers the protection of personal data that have been stored in information systems.

There is also a specific provision in Article 32 that focuses on personal data protection which requires taking measures to protect personal data from unlawful processing or disclosure.

Criminal Procedure Code

As it has been mentioned above, personal data can be processed if this has been provided by law. One of the legislative acts, providing a legal basis for personal data processing is Criminal Procedure Code.

Although the provisions are rather limited, some of the following ones would be of interest.

Pursuant to Article 2, one of the tasks of the CPC is to ensure that the rights and interests of physical persons who could be victims, suspects or accused persons, are being respected during the criminal procedure.

Although CPC Articles 8, 10 and 11 provide for general safeguards related to procedural rights, they do not cover privacy and personal data protection.

CPC Article 13 provides for the protection of private life. Every person has a right to a protection of private life including secrecy of correspondence, phone, and other messages. Measures interfering these rights can be used in accordance with the CPC.

Still, there are no specific provisions on how the personal data is being processed. There are specific provisions related to measures intruding privacy and private life, but the CPC does not contain provisions on overall processing of personal data during and after the criminal proceeding.

Draft law on personal data

At the moment there is no specific law on personal data protection. However, the authorities have prepared a draft law which would introduce personal data protection framework, including standards on data protection as well as supervision.

The aim of the draft law is to introduce definitions and basic principles, rights and obligations related to processing of data as well as supervision mechanism and sanctions.

Draft law introduces the definitions, including for personal data, data processor, processing, cross border transfer etc. There are also specific definitions for biometric personal data, genetic personal data, personal data that is publicly available and special personal data.

The scope of the draft law would cover processing of personal data except for personal use and when related processing of state secrets.

Personal data processing must always be in line with the legislative acts. The basis for the processing would be either consent of the data subject or legislation. The processing must also comply with different principles such as necessity, proportionality, purpose limitation, data minimization etc.

The draft law also provides for rights to data subjects and obligations for data processors.

There is also a separate provision, Article 10, on cross-border data transfers. The transfer is not permitted if there are no sufficient personal data protection standards present. However, there are exceptions which include the consent of the data subject, data can be requested by any

person, data is publicly available, it is done within the framework of an international agreement, transfer is related to a financial monitoring or investigation related to money laundering, financing of terrorism, proliferation of weapons of mass destruction, and las but not least, if the transfer has been permitted by personal data protection authority.

Articles 20, 21 and 22 address the supervision of data protection standards and sanctions related to breaches.

Here the draft law provides for powers and functions of data protection authority which include control and supervision, handling complaints, issuing orders to processors of data, assessing the data protection standards in other countries, giving permissions for cross border data transfers, providing guidance and explanations related to personal data protection as well as participating in the work of international organizations.

Government entities, legal and physical persons are obliged to cooperate with data protection authority and provide to it necessary information.

However, the draft law doesn't specify or establish the data protection authority. Although it provides that the resources necessary will be provided from the state budget, it doesn't designate the authority. Instead it refers that the authority will be designated by the President of the Republic.

The draft law also foresees that the supervision of personal data processing will be conducted by Prosecutor General's Office.

While the draft law introduces the basic definitions and principles related to the personal data protection, there could still be few problems that need to be addressed.

The definitions might go too much into technical details and their added value could be questioned.

There are also questions related to the future data protection authority as it is not established by the law. Giving competence and functions related to the data protection to a criminal justice authority could also cause problems.

Therefore, if there is an intention to bring the domestic data protection framework and legislation in line with relevant CoE and EU instruments, more work and amendments might be needed.

Bringing the legislation in line with relevant international instruments and introducing sufficient data protection regime including independent supervision, would also make international cooperation and information exchange more efficient.

5 Georgia

5.1 Introduction

Georgia has ratified Convention 108 od 12 December 2005.[8] At the time of submitting this study it still has not ratified the Amending Protocol. Legal rules pertaining to personal data protection are found in the following sources of Georgian law:

1. Constitution of Georgia,
2. Law of Georgia on Personal Data Protection, hereinafter: GePDPL
3. Law of Georgia on State Inspector Service, hereinafter: GeSISL
4. Law of Georgia On Electronic Communications, GeECL
5. Law of Georgia On Operative Investigatory Activities, hereinafter: GeOIAL
6. Law of Georgia on Police, hereinafter: GeLPol

5.2 Legislation

Constitution

Article 15 of the Constitution of Georgia provides basic guarantees for personal and family life, personal space, and communication. These rights can be restricted in accordance with the three-step test which corresponds to the one in Article 8(2) of the ECHR, namely that the restriction is (1) in accordance with the law, (2) pursues legitimate aim and (3) is necessary in democratic society. Activities of the LAEs are recognized as legitimate under the constitution. Namely, it allows for restrictions of the rights to privacy and data protection to protect national security, public safety, or for protecting the rights of others. Moreover, Article 15(2) of the Constitution also contains a provision which stipulates that court order is necessary to restrict communication privacy in every individual case. Finally, the same article goes so far as to impose general requirements for interference without court order, in urgent cases.[9] In this context Georgian law is much more privacy-sensitive than in many other jurisdictions, since most countries elaborate procedures and conditions for operations in urgent cases on the level of statutory law.

Law on Personal Data Protection

The Law on Personal Data Protection (GePDPL) is the main source for personal data protection in Georgia. Its material scope is defined broadly in line with the GDPR and includes:

- processing of data through automatic or semi-automatic means, and
- processing of data which form part of the filing system or are intended to form part of the filing system through non-automatic means.[10]

Exceptions to the GePDPL are prescribed in its Article 3(3). In the context relevant for this study, it is important to note that the GePDPL does not transpose fully exception stipulated in Article 2(2)(d) of the GDPR.[11] In other words, GePDPL does not fully exclude activities of LEAs from its

[8] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures (15 July 2020)

[9] Pursuant to Article 15(2) of the Georgian Constitution, in cases of urgent necessity provided for by law fundamental rights can be restricted even without court order. In such cases, "a court shall be notified of the restriction of the right no later than 24 hours after the restriction, and the court shall approve the lawfulness of the restriction no later than 24 hours after the submission of the notification".

[10] Article 3(1) of the GePDPL. Compare with Article 2(1) of the GDPR.

[11] Pursuant to Article 2(2)(d) of the GDPR, *"This Regulation does not apply to the processing of personal data: … (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of*

scope. This is further reinforced by the second sentence in the Article 3(1) of the GePDPL, which stipulates that "*This Law shall also apply to automatic processing of data defined as a state secret for the crime prevention and investigation, operational-investigative activities and protection of the rule of law, except as provided in this article*".

Nevertheless, there are some exceptions for LEAs operations in the GePDPL. Pursuant to its Article 3 paragraph 3, GePDPL does not apply to (in relevant part):

> b) data processing for court proceedings as far as it may prejudice the proceedings before the final decision of the court;
>
> c) processing of the data defined as a state secret for the purposes of state security (including economic security), defence, intelligence and counter-intelligence activities;
>
> d) processing of information defined as a state secret (except for the data specified in paragraph 1 of this article).

Therefore, we see that Georgian law excludes state activities in security, defence, intelligence, and counter-intelligence sector from the scope of general personal data protection rules. It is important to note here that this exception applied only to the extent that personal data which are being processed are defined as "state secret".

On the other hand, LEAs' activities in the sphere of crime prevention, investigation and operational-investigative activities are subject to the GePDPL. Still, there are some restrictions here once again. Namely, pursuant to Article 3(6) of the GePDPL, its Article 6, which regulates legal grounds for processing of special categories of data,

> shall not apply to data processing for public safety, operational and investigative activities and criminal investigations if the issue is directly and specifically regulated under the Criminal Procedure Code of Georgia or the Law of Georgia on Operational and Investigative Activities or other special laws.

It therefore clearly follows that data processing operations for public safety, operational and investigative activities and criminal investigations fall within the scope of the GePDPL, and that only processing of special categories of personal data can be excluded from the scope of this law, if the issue is directly and specifically regulated under the GeCPC or the GeOIAL.

Sectoral legislation also brings data processing operations of the LEAs within the scope of the GePDPL:

- Article 15(3) of the GeLPol prescribes that "*the Police shall process the personal data according to the legislation of Georgia on personal data protection, unless otherwise determined by this Law*".
- Article 6(4^1) of the GeOIAL, dealing with legal guarantees for the protection of human rights and freedoms in operative-investigative activities, stipulates that protocol about deletion of certain sensitive personal data obtained by surveillance of electronic communications shall be submitted to the State Inspector's Office. Similarly, Article 5 of the GeOIAL, dealing with publicity of operative-investigative activities, stipulates that "*Operative-investigative activities are strictly confidential. Only persons defined by this Law, as well as within the framework of the Law of Georgia on the Service of the State Inspector of Georgia, have the right to get acquainted with the data, documents and*

criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

sources reflecting such activities". This is relevant since State Inspector of Georgia monitors lawfulness of personal data processing in general and covert investigative actions and activities performed within the central databank of electronic communications identification data, in particular.[12]

- Law enforcement activities pertaining to video-surveillance in public spaces and in public transport are also subject to the GePDPL.[13]

Therefore, it is evident that the Georgian legislator opted to subject LEAs activities to general data protection law, instead of enacting special law for this purpose. This means that general rules and safeguards defined in the GePDPL are applicable to data processing activities of LEAs unless rules in specific legislation apply.

Legal grounds for data processing are regulated in an exhaustive manner in Article 5 of the GePDPL, which reads as follows:

> Data processing shall be admissible if:
> a) there is a data subject's consent;
> b) data processing is provided for by Law;
> c) data processing is necessary for a data controller to perform his/her statutory duties;
> d) data processing is necessary to protect vital interests of a data subject;
> e) data processing is necessary to protect legitimate interests of a data controller or a third person, except when there is a prevalent interest to protect the rights and freedoms of the data subject;
> f) according to the Law, data are publicly available or a data subject has made them publicly available;
> g) data processing is necessary to protect a significant public interest under the Law;
> h) data processing is necessary to deal with the application of a data subject (to provide services to him/her).

Any procedural power defined in the GeCPC, GeOIAL, GeLPol and other laws, if applied against natural person, will necessarily involve some processing of personal data.

In the context of data processing by LEAs, legal grounds in Article 5 paragraphs b and c are relevant. In particular, data processing which is necessary for a data controller to perform its statutory duties (provision corresponding to Article 6(1)(e) of the GDPR) shall be primarily relevant when other legislation requires LEAs to perform certain duties, while at the same time does not regulate associated data processing activities. For instance, when it becomes necessary to process personal data to perform tasks defined in the GeCPC, GeOIAL, GeLPol and other legislation governing LEAs activities, legal ground in Article 5(c) of the GePDPL is used. This provision should be applied in line with CJEU's interpretation in *Huber* case,[14] pursuant to which (1) only information necessary for the performance of statutory duty should be processed, (2) stored data should, where appropriate, be brought up to date so that they reflect the actual situation of the data subjects, and irrelevant data should be removed and (3) the requirement of necessity is satisfied if the processing of data contributes to the more effective application of other legislation.[15]

Criminal Procedure Code

[12] https://personaldata.ge/en/about-us

[13] See Article 11 of the GePDPL.

[14] Case C-524/06, *Heinz Huber v Bundesrepublik Deutschland*.

[15] *Huber* (cited above), para 58 – 62.

Turning now towards the sectoral legislation, we note that GeCPC contains only several provisions relevant in the context of personal data processing. Articles 4 and 7 of the GeCPC introduce principles of "Inviolability of personal dignity" and "Inviolability of private life in criminal proceedings". Both principles postulate the duty of judges, prosecutors and investigators to protect private life of participants in criminal proceedings. Article 7 in particular prohibits arbitrary and unlawful interference with private life; imposes a duty for officials not to disclose information on a person's personal life and grants any person who has suffered damage as a result of unlawful disclosure about private life or personal data, with the right to be fully indemnified for the damage.

The most relevant parts of the GeCPC are the ones in Chapters XVI and XVI[1], which cover Investigative Actions Related to Computer Data and Covert Investigative Actions in general.

Processing of data in electronic communications sector

As a rule, electronic communication content data and information about the user of that communication are confidential under the law.[16] But, as in any other country, there are some restrictions to this rule, which are considered necessary to enable operations of the LEAs. In a nutshell, Georgian legislation recognizes restrictions to communication privacy in the following cases:

- Obligation of service providers to submit "identification data of electronic communications" (corresponding to "traffic data" in the sense of the [now invalidated] EU Data Retention Directive);
- Execution of special investigative actions, pursuant to 143[1](1)(a, b, c) of the GeCPC;
- In the case of counterintelligence activities.

To facilitate surveillance of communications, the authorized body - Operational-Technical Agency of Georgia - has the right to request from electronic communication companies to enable collection of content and traffic data[17], as well as geolocation data,[18] in real-time. Following the implementation of this capability, Operational-Technical Agency of Georgia can conduct surveillance without further need for technical or legal participation of the electronic communication company.[19] And while the communication service providers must record the facts of transfer of electronic communications identification data[20] to the relevant state bodies and provide relevant information to the State Inspector Service,[21] it remains unclear whether the Operational-Technical Agency possesses technical capability of accessing data without the knowledge of the service providers. This certainly seems possible since GeLEC empowers the Operational-Technical Agency to copy the electronic communication identification databases and keep them in the Central Bank of Electronic Communication Identification Data.[22] This solution can possibly give rise to some concern. As was explained by the ECtHR in *Zakharov* case, "*the requirement to show an interception authorisation to the communications service provider before obtaining access to a person's communications is one of the important safeguards against abuse by the law-enforcement authorities, ensuring that proper authorisation is obtained in all cases of interception*".[23] On the other hand, we do not lose sight from the fact that activities of the Operational-Technical Agency of Georgia are subject to the oversight by the State Inspector Service.

[16] GeECL Article 8(1).

[17] GeECL Article 8[1](1).

[18] GeECL Article 8[4].

[19] GeECL Article 8[1](2).

[20] But there is no corresponding obligation for content and geolocation data.

[21] GeECL Article 8[2].

[22] GeECL Article 8[3](1).

[23] *Roman Zakharov v. Russia*, judgment of 4 December 2015, para 269.

5.3 Data Protection Authority

Since the enactment of the GePDPL, Personal Data Protection Inspector was the authority tasked with monitoring the legality of data processing in Georgia. Following the enactment of the GeSISL Personal Data Protection Inspector was replaced with the State Inspector Service, in May 2019. The Service is headed by the State Inspector, who is elected by the Parliament for a period of 6 years.[24]

State Inspector Service is an independent state body, tasked with controlling (1) the legality of personal data processing in general, and (2) the secret investigative actions and activities implemented in the central bank of electronic communication identification data, in particular. Therefore, State Inspector Service has clear competence to supervise personal data processing activities of LEAs. Its competences are further strengthened by having investigative jurisdiction for certain crimes if they are committed by the representatives of law enforcement body, officers or persons equal to them.[25]

The State Inspector Service has competence over individual applications (request to protect rights) by data subjects in relation to personal data processing, and to take measures provided for by the legislation of Georgia.[26] In executing this task, it is also competent to examine and investigate circumstances as well as request and receive information from any data processor or other authorised person. Likewise, State Inspector Service has competence to conduct inspections, at its own initiative or upon application of an interested person.[27] While the decision on individual application is pending the State Inspector Service can issue temporary measure of blocking data processing.[28] If a violation of data protection rules is detected, The State Inspector Service has competence to issue different corrective measures, as well as to impose administrative penalties.[29]

State Inspector Service's competences in monitoring legality of LEAs are subject to special set of provisions in the GeSISL.[30] In particular, the State Inspector Service is empowered to monitor operations of LEAs in obtaining computer and other data, including:

- Investigative actions pertaining to production of data, real-time collection of traffic data and interception of content data.[31] This is achieved by collation of information from courts, the Prosecutor's Office, an electronic communication service provider as well as by conducting inspections.
- Secret investigative actions of telephone bugging and recording, by controlling the legality of data processing via electronic control system, and by conducting inspections of data processor or other authorized person.[32]
- Secret investigative actions of the retrieval and recording of information from a communications channels and computer systems,[33] by conducting inspections.

[24] GeSISL, Article 6.

[25] GeSISL, Article 19(1).

[26] GeSISL Article 14.

[27] GeSISL Article 15

[28] Data processing for state security and defence purposes is exempted from this.

[29] GeSISL Article 16.

[30] GeSISL Article 18.

[31] GeSISL Article 18(2), in relation to GeCPC Articles 136 – 138.

[32] GeSISL Article 18(1), in relation to GECPC Article 143[1](1)(a).

[33] GeSISL Article 18(3), in relation to GeCPC Article 1431(1)(b).

- Secret investigative actions of real-time geolocation identification,[34] by monitoring through a special electronic control system and by conducting inspections.
- Activities carried out in the central bank of electronic communication identification data, through the electronic control system of central bank of electronic communication identification data and through the inspections.[35]

[34] GeSISL Article 18(5), in relation to GeCPC Article 1431(1)(c).

[35] GeSISL Article 18(6).

6 Moldova

6.1 Introduction

Moldova ratified Convention 108 on 28 February 2008. Amending Protocol has not been signed yet. Personal data protection is regulated by the Constitution, Law on Protection of Personal Data (hereinafter: MdLPPD) and some sectoral legislation.

6.2 Legislation

Constitution

Moldovan Constitution does not contain any provisions dealing specifically with personal data protection. Looking more broadly, guarantees of protection of private and family life[36] and privacy of correspondence[37] are relevant. These rights can be restricted in particular cases, under the following conditions: (1) restriction must be provided by law, (2) it must pursue one of the legitimate aims enumerated in the Constitution and (3) it must be proportionate to the situation and must not affect the existence of the right or freedom.[38]

Law on Protection of Personal Data

Moldovan Law on Protection of Personal Data (MdLPPD) was enacted in 2011. One of the declared aims of this statute was to ensure compliance with the EU Directive 95/46. This is visible throughout the text, which uses the structure and provisions corresponding to the directive.

Regarding the scope of this law, it is important to note that it is specifically prescribed in the MdLPPD that its scope of application includes "*processing of personal data within the actions of prevention and investigation of crimes, the execution of convictions and other actions within the criminal or contravention procedure under the law*".[39] Moreover, pursuant to Article 2(4)b, MdLPPD continues to apply in this context, even if personal data are considered state secret. Therefore, it is obvious that Moldovan legislator opted for full application of personal data protection law in the criminal law area. On the other hand, MdLPPD contains an interesting exception not found elsewhere, namely that it does not apply to "*the processing operations and cross-border transmission of personal data referring to the perpetrators or victims of genocide, crimes against humanity and war crimes*".[40]

MdLPPD is also compatible in the high degree with the Directive 95/46 when it comes to data processing principles,[41] legal grounds for data processing[42] and special categories of data.[43]

Article 8 of the MdLPPD addresses processing of personal data related to convictions criminal proceedings, coercive procedural measures or sanctions for minor offenses. In a nutshell, it is stipulated that these processing operations can be performed only by or under the control of public authorities in accordance with specific laws governing those activities. Moreover, it is

[36] Constitution of the Republic of Moldova, Article 28.

[37] *Ibid*, Article 30.

[38] *Ibid*, Article 54 paragraphs 2 and 4.

[39] MdLPPD, Article 2(2)d

[40] MdLPPD, Article 2(4)c

[41] MdLPPD, Article 4.

[42] MdLPPD, Article 5.

[43] MdLPPD, Article 6.

prescribed that Ministry of Internal Affairs is authorized to process data containing forensic and criminological information.

Rights of the data subject are also regulated in a manner compatible with the Directive 95/46.[44]

Criminal Procedure Code

Criminal Procedure Code of Moldova (MdCPC) is relatively silent when it comes to personal data protection provisions. In general terms, some principles of criminal procedure are relevant here.

Firstly, principle of inviolability of private life calls for, intel alia, protection of information on private and intimate life. Pursuant to Article 15(2) of the MdCPC, such information may not be collected unless necessary. We note here that the concept of "information on private and intimate life", used in the MdCPC, is not synonymous with the notion of "personal data" (later being the broader one). However, it seems that not much substance is lost here, since Article 15(2) of the MdCPC also explicitly stipulates that the data of personal nature shall be processed during criminal proceedings in line with the provisions of the MdLPPD.

Secondly, Article 14 of the MdCPC prescribes that privacy of correspondence is also one of fundamental principles of criminal procedure, and can only be limited on the basis of legal warrant issued on the basis of that code.

Next, it is stipulated in Article 303 that investigative measures related to limiting person's private life are considered to be "special", with the consequence that additional conditions and safeguards are applicable to them.

6.3 Data Protection Authority

Pursuant to Article 19 of the MdLPPD, National Center for Personal Data Protection (NCPDP) is given the role of data protection authority. It is provided with broad competences, including monitoring application of data protection legislation, issuing necessary instructions to ensure legality of data processing, issuing orders to suspend or cease unlawful processing of data, maintains register of data processing operations, cooperates with other stakeholders from public and private sector, etc.[45] In ensuring compliance with data protection legislation, the NCPDP is authorized to request and receive information, use expert assistance and order rectification, blocking or destruction of unlawful or incorrect personal data.[46]

[44] MdLPPD, Articles 12 – 18.

[45] MdLPPD, Article 20(1).

[46] MdLPPD, Article 20(2).

7 Ukraine

7.1 Introduction

Ukraine has ratified the Convention 108 on 30 September 2010. Amending Protocol hasn't been signed yet.

Standards related to protection of personal data have been provided by the Constitution of Ukraine and Law on Protection of Personal Data.

The Ombudsman on Human Rights acts also as data protection authority.

7.2 Legislation

The Constitution

The basic constitutional guarantees on privacy and personal data have been provided by Articles 31 and 32.

Article 31 protects the privacy and secrecy of communications.

Article 32 protects individuals from interference with personal and family life. The processing of information about a person cannot take place without the consent except cases provided by the legislation. Individuals have also a right to access and examine information about themselves unless there are limitations related to state or other secrets. The Constitution also guarantees a right to demand the data corrected or deleted as well as a right to compensation for damages.

Criminal Procedure Code

While there is no specific provision on data protection and processing of personal data, still general procedural safeguards apply.

Pursuant to Article 7 criminal proceedings must also comply with non-interference with private life.

Article 9 on legality of proceedings refers also to requirements of the Constitution, other laws and international treaties that Ukraine is party to. There is also a reference to a case law of the European Court of Human Rights that needs to be taken into account while applying the criminal procedure legislation.

Article 14 provides safeguards related to the confidentiality of communications. Article 15 guarantees everyone the non-interference with private life and requires that personal data may be processed only with the consent of the person, except cases provided by the CPC. There is also a purpose limitation clause according to which the information collected can only be used for the purpose of criminal proceeding. Also, information on private life that has been collected has to be kept confidential and prevent its disclosure.

Protection of private life has also been provided by Article 27 according to which the court proceedings may take place *in camera*. This applies also to the pronouncement of court decisions. If the trial has been closed to public then decisions are not pronounced publicly.

Law on Protection of Personal Data

The scope of the law covers processing of personal data except for personal or domestic needs. It also excludes data processing related to creative, literature or journalist professions. However, it must be ensured that the appropriate balance is ensured between right to privacy and right to freedom of expression.

Article 2 provides for the basic definitions such as personal data, controller and processor, consent and depersonalization.

Article 6 introduces the principles for the processing of personal data including open and transparent processing, data quality, necessity and proportionality as well as purpose limitation.

Processing of personal data may take place on the basis of consent or if prescribed by the legislation.

Purpose has to be always clearly formulated in legislative acts or other documents. In case the purpose changes, the data subject needs to provide new permission or consent.

Primary source for personal data should be the data subject itself. Data needs to be accurate, authentic and updated when necessary.

Article 7 contains are also specific requirements with regard to particular personal data such as about racial or ethnic origin, political views, religion, membership in political parties and trade unions, criminal charges and convictions, as well as data related to health or sexual life.

In this case the processing is allowed if the consent has been given by the data subject or if other ground provided by the law are present. One of the exceptions provided is also related to criminal proceedings and enables processing of personal data for criminal justice purposes, counterintelligence and antiterrorism activities.

The also provides for the rights of the data subject as well as obligations for data processor and data controller.

While there are already exceptions for personal data processing when prescribed by the legislation, Article 25 provides also additional limitations.

Pursuant to Article 25 rights of the data subject can be restricted for the purposes of national safety, economic welfare and human rights, to protect other individuals and for anti-criminal activity.

Article 29 provides the conditions for cross-border transfer of data. The transfer is allowed only if provided by law or international agreement and if relevant country has an adequate level of personal data protection. However, member states of the European Economic Area and signatories to the Convention 108 are always assumed to have adequate standards in place.

As regards other countries, it is the task of the Cabinet of Ministers to compile a list of countries that are considered as adequate.

There are also additional conditions in place concerning the rest and personal data may be transferred also if there is explicit consent of the data subject or in cases where there is a need to protect vital interests of data subjects or need to protect public interests. In this case a personal data controller has to provide required guarantees related to the non-intrusion into the private and family life of the data subject.

However, in this case there is no requirement to consult or seek a permission from the DPA.

7.3 Data protection authority

Pursuant to the Article 22 of the law, the control and supervision are the task of the state bodies and Ombudsman of the Verkhovna Rada on human rights matters.

The powers and functions have been provided by the law and the authority exercises them independently

The DPA ensures inter alia the performance of state policy in the sphere of personal data protection, controls and supervises the application of legislation, conducts both remote and onsite inspections, investigates the violations, handles complaints and participates in the work of international organizations dealing with personal data protection.

The DPA provides also guidance on personal data protection requirements and issues regulations.

8 Conclusions

Most countries analysed in this report provide some protection to personal data on the constitutional level. However, there are many differences in the approach here. In particular, most countries rely on general provisions providing protection to private and family life, including communication, and do not have special rules addressing specifically personal data. Exceptions are Armenia and Azerbaijan, whose constitutions do treat personal data explicitly. In all countries except Belarus, limitations of fundamental rights are subject to the usual three-step approach used in Article 8 of the ECHR. Also, the needs of law enforcement, both in criminal law as well as in national security area, can serve as a legal basis for use of personal data.

As regards the countries that are being analysed in this report, all of them except Belarus are parties to the Convention 108. This means that Armenia, Azerbaijan, Georgia, Moldova, and Ukraine have undertaken international obligations to establish adequate personal data protection framework and designate independent supervisory body. Being a state party to the Convention 108 also means that data transfers may take place between these countries as well as between other parties to the Convention 108.

While the analysis of compliance with the Convention 108 would be outside of the scope of this study, it is obvious that in most countries additional efforts would be needed to ensure harmonization with that Convention. We note with satisfaction that some countries also seek to implement relevant EU legislation, whether the GDPR (as in the case of Georgia) or earlier Directive 95/46 (as in the case of Moldova).

Law enforcement activities and criminal justice have been recognised as a legal ground for the processing of personal data. Therefore, instead of a consent of a data subject, the data processing is based on special law. Although law enforcement activities and criminal justice are generally recognised as legal grounds for data processing, the domestic legislation often doesn't provide that. In this context we note that there are very limited references, or no references at all, to personal data protection rules and related obligations in domestic Criminal Procedure Codes. Certain aspects are covered by general provisions and procedural safeguards, but usually there are no specific provisions dealing with various aspects of data processing.

Legislation of countries we analysed in this report is usually most developed in relation to special operative-investigative measures, and in particular those which pertain to surveillance of communications (see for instance Georgia).

Cross-border data transfers are becoming more and more crucial. As regards criminal investigations, often electronic evidence or computer data is being stored or available abroad. By sending a request to another country, international organisation or multinational service provider, personal data is also being transferred. Same would apply for sending replies to requests received from abroad.

If the receiving country has adequate personal data protection standards in place, data in principle could be transmitted. However, if it is not the case, too rigid and limited domestic legislation could pose problems. Therefore, certain exceptions could be beneficial, which would enable efficient international cooperation.

At the moment, only Armenia has signed the Amending Protocol to the Convention 108. The Amending Protocol will raise the data protection standards and make them comparable to the EU GDPR framework. However, there is no information available on the plans and next steps with regard to the Amending Protocol.

As data protection standards and related safeguards will continue to play a big role concerning international cooperation, countries should consider to take necessary measures and amend domestic legislation accordingly.

This would enhance cooperation not only with EU Member States that are already now bound by the GDPR, but also with other countries.

As of July 2020, the negotiations on the 2nd Additional Protocol to the Budapest Convention take place. The Protocol would introduce additional measures and tools for the law enforcement, including on direct cooperation with multinational service providers. One of the cornerstones of the Protocol are provisions and safeguards on data protection.

This is also one aspect that states need to bear in mind and therefore need to work in order to keep their data protection frameworks up to date.